May 6, 2011

VIA EMAIL AND HAND DELIVERY

The Honorable Greg Walden
Chairman
Subcommittee on Communications and Technology
United States House of Representatives
Washington, DC 20515

Dear Chairman Walden:

Apple provides this letter in response to the Committee's letter of April 25, 2011.

On April 27, 2011, Apple issued the attached public response to questions about how Apple gathers and uses location information. That response provides much of the information requested in your letter. The following summary provides additional details regarding Apple's collection, storage, and use of location information on Apple mobile devices. After this summary, specific answers are given to each question in your letter.

At the outset, the initial point made in Apple's April 27 public response should be emphasized: Apple does not track users' locations – Apple has never done so and has no plans to ever do so. Instead, to provide the best services to meet customers' demands, Apple collects the following, limited kinds of location-related information from a device.

I. **SUMMARY OF APPLE'S COLLECTION, STORAGE, AND USE OF LOCATION INFORMATION ON APPLE MOBILE DEVICES**

A. **Crowd-Sourced Database of Wi-Fi Hotspot and Cell Tower Location Information**

Consumers are increasingly demanding accurate location information from their handheld devices. Consumers want directions from their current location to a desired destination; consumers want their devices to find the nearest coffee shop or gas station. To get this type of information, consumers want and expect their mobile devices to be able to quickly and reliably determine their current locations. If the device contains a GPS chip, the device can determine its current location using GPS satellite data. But this process can take up to several minutes. Obviously, if the device does not have a GPS chip, the GPS location data is not available at all.

To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer's request for current location information, Apple maintains a secure database containing

1

information regarding known locations of cell towers and Wi-Fi access points – also referred to as Wi-Fi hotspots. (For additional details, please see Apple's July 12, 2010 Letter to The Honorable Edward J. Markey and The Honorable Joe Barton (Apple's "July 12, 2010 Letter") at 6.)[1] As described in greater detail below with regard to mobile devices – and as discussed in detail with regard to both mobile devices and Mac computers in the July 12, 2010 Letter – Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of Apple devices. From this anonymous information, Apple has been able, over time, to calculate the known locations of millions of Wi-Fi hot spots and cell towers. Because the basis for this location information is the "crowd" of Apple devices, Apple refers to this as its "crowd-sourced" database. The crowd-sourced database does not reveal personal information about any customer.

An Apple mobile device running Apple's mobile device operating system, iOS, can use the crowd-sourced database to (1) provide the customer with an approximate location while waiting for the more precise GPS location, (2) find GPS satellites much more quickly, significantly reducing the wait time for the GPS location, and (3) triangulate the device location when GPS is not available (such as indoors or in basements). The device performs all of these calculations in response to a request for location information from an application on the customer's device that has been explicitly approved by the user to obtain the current location, and the device requests from Apple the crowd-sourced database information needed for these calculations.

To further improve the speed with which the device can calculate location, Apple downloads a subset of the crowd-sourced database content to a local cache on the device. This content describes the known locations of Wi-Fi hotspots[2] and cell towers that the device can "see" and/or that are nearby, as well as nearby cell location area codes,[3] some of which may be more than one hundred miles away. The presence of the local cache on the device enables the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

As discussed in more detail below, Apple issued a free software update that changed the way in which iOS maintained its local cache. The software update reduced the size of the crowd-sourced Wi-Fi hotspot and cell tower database cached on the devices, ceased backing up this cache, and deleted the cache entirely when Location Services is off.

For devices that have installed this update, iOS stores this local cache in a database file called "cache.db." For devices running previous versions of iOS 4, iOS stores this local cache in the "consolidated.db" database. Except as otherwise noted, "local cache" is used herein to refer to the downloaded hotspot and cell tower location information, whether stored in consolidated.db or in cache.db.

---

[1] For your reference, a copy of Apple's July 12, 2010 Letter is attached and is also available online on Congressman Markey's website at http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf.
[2] For each Wi-Fi hotspot, the location information includes that hotspot's MAC address, latitude/longitude coordinates, associated horizontal accuracy number, and a confidence value. For each cell tower, the location information includes the cell tower ID, latitude/longitude coordinates, associated horizontal accuracy number, and a confidence value.
[3] Cell base stations are grouped into "location areas" for network planning purposes, and each location area is assigned a unique "location area code." This "location area code" is broadcast by the cell base stations.

The local cache does not include a log of each time the device was near a particular hotspot or cell tower, and the local cache has never included such a log. For each Wi-Fi hotspot and cell tower, the local cache stores only that hotspot's/cell tower's most recent location information, downloaded from Apple's constantly updated crowd-sourced database. After a customer installs the free iOS software update, iOS will purge records that are older than seven days, and the cache will be deleted entirely when Location Services is turned off.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

When a customer runs certain applications, those applications request location information from iOS. Because of a bug that existed prior to the update, even when Location Services was off, the device would anonymously send the IDs of visible Wi-Fi hotspots and cell towers, without any GPS information, to Apple's servers, Apple's servers would send back the known, crowd-sourced location information for those hotspots and cell towers (and nearby hotspots and cell towers), and the device would cache that information in the consolidated.db file. None of this downloaded crowd-sourced location information – or any other location information – would be provided to or disclosed to the application.

The iOS software update fixed the bug that caused crowd-sourced location information to be downloaded to the device while Location Services was off. iOS will now delete any existing local cache from consolidated.db and, if Location Services is off, (1) Apple will not download any crowd-sourced location information to the device, regardless of whether a specific application requests that information, and (2) iOS will delete any cache of this information stored in cache.db.

B.   Collecting Crowd-Sourced Wi-Fi Hotspot and Cell Tower Location Information

As mentioned above and in the July 12, 2010 Letter, Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of devices to develop and refine Apple's database of crowd-sourced location information. The mobile devices intermittently collect information about Wi-Fi hotspots and cell towers that they can "see" and tag that information with the device's current GPS coordinates, i.e. the devices "geo-tag" hotspots and towers.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a separate table in the local cache; thereafter, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection every twelve hours (or later if the device does not have Wi-Fi access at that time). Apple's servers use this information to re-

calculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced database. As explained in Apple's April 27 public response and Apple's July 12, 2010 Letter, Apple cannot identify the source of this information, and Apple collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced database. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one application's request to use location information.[4]

C.   Additional Location Information Collections

If Location Services is on, Apple collects location information from mobile devices under the following additional circumstances.

First, as mentioned in Apple's April 27 response, Apple is now collecting anonymous traffic data to build a crowd-sourced automobile traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years. This information is temporarily stored in the local cache on the device, anonymously uploaded to Apple, and then deleted from the device.

Second, Apple collects anonymous diagnostic information from randomly-selected devices to evaluate and improve the performance of its mobile hardware and operating system. For example, Apple may collect information about a dropped cell phone call, including the calculated location of the device when a call was dropped, to help identify and address any cell connection issues. Before any diagnostic information is collected, the customer must provide express consent to Apple. Apple cannot associate this information with a particular customer. Additional details regarding Apple's diagnostic collection practices are provided in the July 12, 2010 Letter at page 8.

Third, Apple obtains information about the device's location (the latitude/longitude coordinates) when an ad request is made. The device securely transmits this information to the Apple iAd servers, the iAd servers immediately convert the latitude/longitude coordinates to a five-digit zip code, and the iAd servers then discard the coordinates. Apple does not record or store the latitude/longitude coordinates – Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer. Additional details regarding Apple's advertising collection practices are provided in the July 12, 2010 Letter at pages 9-10.

Finally, if a customer has consented to an application's collection and/or use of location information, iOS will provide current location information in response to a request from that application. iOS will provide that customer-approved application with the location of the device only; iOS does not provide applications with direct access to the local cache.

---

[4] When Apple released iOS 4.1 on September 8, 2010, Apple fixed a bug that had caused iOS to send anonymous, geo-tagged information about Wi-Fi hotspots and cell towers to Apple even if the customer had turned off Location Services. For devices running iOS version 4.1 and later, the device does not send this anonymous location information to Apple.

D.   Apple's May 4, 2011 iOS Software Update

As discussed above, Apple released an iOS Software Update. After a customer installs this software update on an iOS device:

- if Location Services is off, Apple will not download any crowd-sourced Wi-Fi hotspot and cell tower location information to the device, regardless of whether a specific application requests that information;

- iOS will delete from consolidated.db any cached location information described above – even if Location Services is on;

- iOS will store cached location information, as described above, in cache.db only if Location Services is on and will delete any such cached location information from cache.db if Location Services is turned off;

- iOS will purge from cache.db crowd-sourced Wi-Fi hotspot and cell tower location information records that are older than seven days; and

- iTunes will not back up cache.db.

II.   RESPONSES

The following responses represent the current state of our knowledge based on our investigation to date. Our investigation is ongoing, however, and we may continue to discover information responsive to your letter. I will update our responses, as needed, if we locate other responsive materials or information.

1.   What location data do devices running your operating system track, use, store, or share?

Under the circumstances detailed above, Apple's mobile operating system, iOS, collects and temporarily stores in a local cache database on the device: (1) location data for Wi-Fi hotspots and cell towers and (2) location data associated with automobile traffic data. In versions of iOS 4 prior to the update, this local cache database is contained in a file named consolidated.db; for devices that have installed the software update, the local cache database is contained in a file named cache.db. Also described above, iOS may collect and temporarily store in files on the device location data associated with diagnostic information. Finally, iOS also collects, but does not store, the device's latitude and longitude coordinates when an ad request is made.

Also as described above, Apple has compiled and updates a crowd-sourced database of location information for Wi-Fi hotspots and cell towers that is derived in part from the geo-tagged hotspot and cell tower information sent by Apple devices. Apple maintains this database on its servers, and Apple downloads a subset of the derived hotspot and cell tower location information to the local cache database on mobile devices. Although this data is stored on the iOS-based mobile device, it is not the data collected from that device or any other device – instead, it comprises the locations for hotspots and cell towers as calculated by Apple.

In versions of iOS 4 prior to the May 4, 2011 software update, iOS wrote a cache copy of the device's single "last known location" to a file named "cache.plist." Specifically, when the device determined its current location, iOS wrote that location to cache.plist, overwriting any previous data that may have been in the file. In other words, only one last known location was stored; previous locations, or locations over time, were not stored by iOS. The next time an application or service requested current location information, iOS used the data in cache.plist, along with other information, to determine the device's then-current location. Any previous location in cache.plist was then overwritten. After the software update is installed on a device, iOS no longer writes the last known location to a file and deletes any last known location stored in cache.plist.

Apple's Mac computers and laptops run Apple's Mac OS X operating system. Mac OS X anonymously collects information about Wi-Fi hotpots, such as MAC addresses. Additional details regarding the collection of this information from Mac OS X are provided in the July 12, 2010 Letter at pages 7-8.

Further, in addition to Apple's operating systems, applications running on Apple devices may also collect and store location information when the customer consents. The details regarding the restrictions placed on applications' collection and use of location information are discussed below.

2. Why does the device track, use, store, or share that data?

Apple and Apple devices collect location-based information for only one purpose – to enhance and improve the services we can offer to our customers.

As discussed above, Apple uses the anonymous, geo-tagged information about Wi-Fi hotspots and cell towers collected from mobile devices, along with other information (such as cellular specifications), to calculate the locations of hotspots and cell towers. Apple stores the calculated locations in Apple's crowd-sourced database. Information from this database enables Apple mobile devices to calculate location quickly (or at all, in the case of non-GPS enabled devices) to the customer's request for current location information.

Apple is using location information associated with automobile traffic data collected from mobile devices to build a crowd-sourced traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years.

Apple uses location information associated with diagnostic data collected from mobile devices to evaluate and improve the performance of its mobile hardware and operating system.

Apple uses location information collected when an ad request is made to calculate a zip code that is used to select a relevant ad for the customer. As noted above, Apple discards the actual location information transmitted from the device to Apple's iAd servers when an ad request is made.

Finally, if a customer has consented to an application's or advertisement's request to use location-based information, iOS will give that application or advertisement the device's current

location. The application or advertisement will not, however, be given direct access to Apple's crowd-sourced database of hotspot and cell tower locations.

3.   Where on the device is the data stored; how is it used, stored, or shared; and how is it protected?

Please see response to Request Nos. 1 and 2.

As discussed above, iOS creates a cache.db local cache database on devices that (1) have installed the software update and (2) have Location Services on. iTunes does not back up cache.db. And if the customer turns off Location Services, iOS will delete any existing cache of the hotspot and cell tower location information from cache.db. In addition, as noted above, when the software update is installed, iOS will delete any existing local cache from consolidated.db (even if Location Services is on).

Also as discussed above, iOS creates files on Apple mobile devices in which geo-tagged diagnostic information may be stored; iTunes does not back up these files.

In versions of iOS 4 prior to the update, the consolidated.db local cache database contained location information as described above. For non-updated devices, if the customer (1) had established a syncing relationship between the customer's mobile device and a personal computer and (2) connected the Apple mobile device to that personal computer, iTunes would back up consolidated.db, including location information, as part of the normal device backup. The iTunes backup, including consolidated.db, may or may not be encrypted, depending on the customer's settings in iTunes. On devices that have not installed the software update, iOS also creates the cache.plist file containing the last known location of the device. This last known location cache is not backed up by iTunes. On devices that have installed the update, iOS will no longer write the last known location to a file and will delete any existing last known location stored in cache.plist.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

4.   How is that data accessible and who can access it? Is the data automatically transferred to your company or to other devices, or to third parties? If so, how and why? Is there any other manner in which data can be transferred or obtained by your company, or by other devices, or by third parties, and if so, how and why?

As described above, versions of iOS 4 transmit anonymously the following categories of location-based information to Apple's servers: (1) geo-tagged information for Wi-Fi hotspots and cell towers; (2) location information associated with automobile traffic data; (3) location information associated with diagnostic data; and (4) in the case of the iAd network, latitude/longitude coordinates for a device when an ad request is made.

Apple has also downloaded portions of the contents of the crowd-sourced database to Apple mobile devices to provide location services to Apple's customers. As discussed above,

the hotspot and cell tower location information stored in Apple's crowd-sourced database and downloaded to customer devices is not the anonymous geo-tagged information collected from mobile devices – instead, it comprises the locations of hotspots and cell towers that have been derived by Apple from the anonymous crowd-sourced location data.

If – and only if – a customer expressly consents to a request for location information made by an application or by an advertisement (for example, to locate the Target store nearest the customer) that has been delivered to the device by Apple's iAd servers, iOS will give that application or advertisement the current location of the customer device. The application or advertisement will not, however, be given direct access to Apple's crowd-sourced database of hotspot and cell tower locations.

Third-party application developers must register as an "Apple Developer" by paying a fee and signing the Registered Apple Developer Agreement and the iOS Developer Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application;

- Developers must provide information to their customers regarding the use and disclosure of location-based information (*e.g.*, a description on the App Store or adding a link to the applicable privacy policy);

- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access;

- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information;

- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;

- If the customer denies or withdraws consent, applications may not collect, transmit, maintain, process or utilize the customer's location data; and

- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions. In its Privacy Policy, Apple also notifies customers that "Information collected by

third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties."

Finally, with the goal of providing its customers with an improved traffic service, Apple has entered into a confidential relationship with one of its development partners and has shared with this partner subsets of the anonymous location information associated with automobile traffic data collected by Apple. Contractual confidentiality and non-disclosure restrictions protect this anonymous location information, and Apple's development partner is prohibited from sharing this information with any third parties. The terms of Apple's agreement with this development partner are confidential.

Other than as described in the prior paragraphs, Apple has not shared or given third parties access to the information collected and stored by iOS.

5. Is the user informed of, or given an opportunity to prevent, such tracking, use, storing, or sharing of data and, if so, how? Can the end-user disable the tracking, use, storing, and sharing of such data? Can the user delete the data?

Apple has publicly disclosed in several ways the types of information it collects and how it uses that information. Through its Privacy Policy and previous disclosures to questions raised about location based data, Apple has informed its customers of the types of data collected and used by the devices. Apple provided a detailed description of its collection and use of location-based information in the July 27, 2010 Letter. In Apple's April 27, 2011 public response, Apple disclosed additional technical details, including characteristics of the local cache database file.

Apple has taken several measures to inform its customers about the use of location data. First, Apple's Privacy Policy, which is available from links on every page of Apple's website,[5] contains express disclosures regarding Apple's collection and use of location data and non-personal information:

---

[5] The links take customers to http://www.apple.com/privacy, which may also be accessed by customers directly.

Location-Based Services

To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.

Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

****

Collection and Use of Non-Personal Information

We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

- We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

...

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

Second, Apple's Software License Agreements ("SLAs") for products that provide location-based services similarly provide express disclosures regarding Apple's collection and use of location information. For example, to activate an iPhone, the customer must accept and agree to the iPhone SLA, including the following provision regarding location data:

4.   Consent to Use of Data.

...

(b) Location Data. Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide and improve these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide and improve location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** (emphasis exists in the SLA) You may withdraw this consent at any time by going to the Location Services setting on your iPhone and either turning off the global Location Services setting or turning off the individual location settings of each location-aware application on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services. ...

At all times your information will be treated in accordance with Apple's Privacy Policy, which is incorporated by reference into this License and can be viewed at: www.apple.com/legal/privacy/.

In addition, every time a customer updates iOS on an iPhone, the customer must again accept and agree to the iPhone SLA.

Third, before any application can collect or use location information, iOS discloses to the customer that the application "would like to use [the customer's] current location" and requests the customer's express consent.

Fourth, before Apple will collect any diagnostic information from an iOS customer, that customer must explicitly agree that Apple may collect and use such information. For example, iPhone customers must click "Agree" in response to the following disclosure:

11

You can help Apple improve its products by sending us anonymous diagnostic and usage information about your iPhone.

By clicking "Agree" you agree that Apple may periodically collect and use this information as part of its support services and to improve its products and services. This information is collected anonymously. To learn more about Apple's Privacy Policy, see http://www.apple.com/legal/privacy.

In addition, Apple has always provided its customers with functionality to control the location-based service capabilities of their devices.

First, Apple has always required express customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," iOS will not provide any location-based information to the application. This dialog box is mandatory—neither Apple's applications nor those of third-parties are permitted to override the notification.

Second, iOS also permits customers to identify individual applications that may not access location-based information, even if Location Services is on. The Location Services settings menu provides an "On/Off" toggle switch for each application that has requested location-based information.
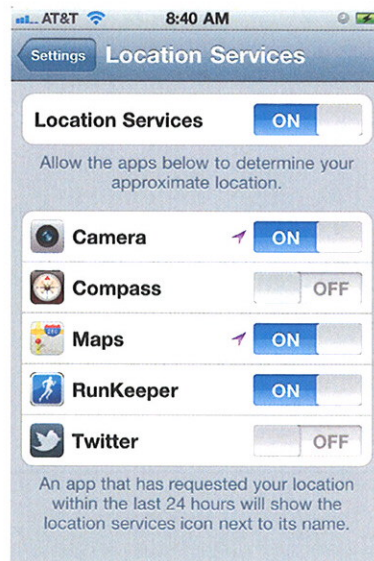

The first time an application requests location-based information, iOS presents the customer with the "Don't Allow/OK" dialog box to request confirmation from the customer. For example, shown below are the dialog boxes iOS presents for the Maps and Camera applications.
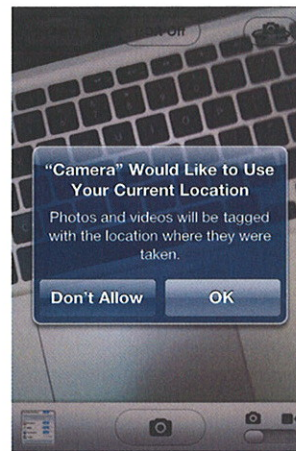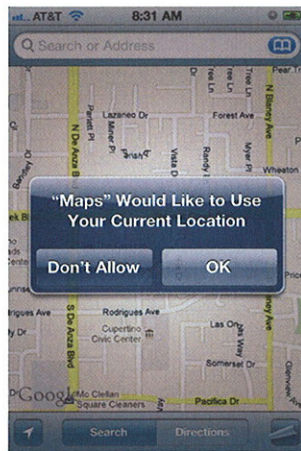
If the customer selects "OK," iOS will list the application in the Location Services setting menu with the "On" setting. If the customer selects "Don't Allow," iOS will list the application with the "Off" setting. When the switch for a particular application is toggled "Off," no location-based information will be provided to that application.

Third, Customers can change their individual application settings at any time. An arrow icon ( ) alerts customers that an application is using or has recently used location-based information. This icon appears in real-time for currently running applications and next to the "On/Off" toggle switch for any application that has used location-based information in the past twenty-four hours.

Fourth, customers can use Restrictions, also known as Parental Controls, on a mobile device to prevent access to specific features, including Location Services. When a customer enables Restrictions, the customer must enter a passcode (this passcode is separate from the device passcode that the customer may set).
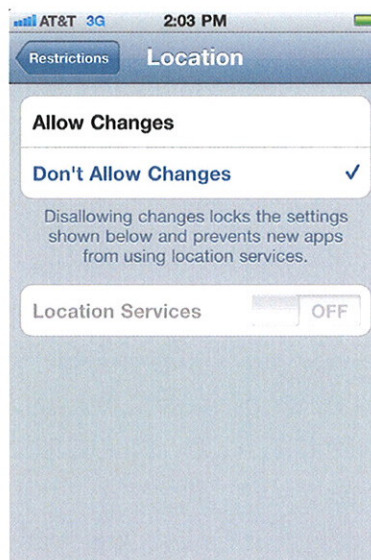
If the customer turns Location Services off and selects "Don't Allow Changes," the user of the device cannot turn on Location Services without that passcode. In addition, (1) iOS will not provide any location information to any applications, including applications that may have previously received consent to use location information; (2) iOS will not collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; and (3) iOS will not upload any location information to Apple from the device.

Finally, for iOS versions 4.1 and later, if the customer turns Location Services off, the mobile device does not send geo-tagged data about Wi-Fi hotspots and cell towers to Apple.

6. How long does the device store the data?

As described above, iOS stores a local cache of crowd-sourced location information about Wi-Fi hotspots and cell towers calculated by Apple. Following the software update, iOS purges records in this cache that are older than seven days and will delete the cached information entirely when Location Services is off.

7. Section 222 of the Communications Act contains privacy provisions. Do those provision apply to you? Should they? Does it make sense that similar information is afforded different privacy protections depending on what entity does the collecting and what service the data is collected from, especially since the entities collecting such information are increasingly competing each other in today's information age?

While Apple is not a telecommunications carrier or service provider subject to Section 222 of the Communications Act, we believe the privacy protections described in detail in this letter are consistent with the intent of Section 222.

8. In a July 12, 2010, response to a June 24, 2010, letter from Reps. Joe Barton and Edward Markey, both of which we attach to this letter, you outlined some of your location data collection practices and privacy protections. Are your current location data collection practices the same as the practices you described in your July 12, 2010, letter? If not, how have those practices changed, and have you notified consumers and Congress of those changes?

As described above, Apple released a software update on May 4, 2011, to address a bug about which Apple was not aware when it provided the July 12, 2010 Letter. Apple described this bug and the software update that addresses the bug in Apple's April 27, 2011 public response.

In addition, when Apple released iOS 4.1 on September 8, 2010, Apple fixed a bug that had caused iOS to send anonymous, geo-tagged information about Wi-Fi hotspots and cell towers to Apple even if the customer had turned off Location Services. For devices running iOS version 4.1 and later, the device does not send this anonymous location information to Apple.

9. **Are you currently planning to implement any measures to address the privacy concerns referenced above?**

We believe our privacy protections, as described above, address the privacy concerns referenced in the Committee's letter.

Sincerely,

Bruce Sewell
General Counsel and Senior Vice
President of Legal and Government
Affairs

Attachments

cc: The Honorable Anna G. Eshoo, Ranking Member
Subcommittee on Communications and Technology